ARTICLE APPEARED
ON PAGE 1

BOSTON GLOBE
5 December 1985

Technology brings fears of an era of Big Brother

"He knew that for seven years the Thought Police had watched him like a beetle under a magnifying glass. There was no physical act, no word spoken aloud, that they had not noticed, no train of thought that they had not been able to infer."
– The novel "1984"

By Ross Gelbspan
Globe Staff

In conferences and publications last year, Americans celebrated the fact that the United States in 1984 had not succumbed to the pervasive state surveillance that George Orwell had detailed in 1949 when his book was published.

But today a growing number of commentators say that a technologically driven explosion of space-age surveillance devices may be bringing a similar scenario much closer to reality than most people believe.

"Technical innovations [in surveillance] have . . . become penetrating and intrusive in ways that previously were imagined only in science fiction," notes sociology professor Gary T. Marx of MIT's urban studies department.

Just 10 years ago, most surveillance consisted of court-approved wiretaps, video cameras in sensitive areas and airport metal detectors.

By contrast, a survey last month of 35 federal agencies by the Congressional Office of Technology Assessment found that government officials are currently using or planning to use such surveillance devices as:

- Massive computerized databases capable of tracking individuals' transactions and activities.
- "Starlight scope" systems to watch people at night.
- Helicopter and satellite cameras to identify people in crowds and track individuals.
- A profusion of remote listening and recording devices, such as miniaturized bugs and remote parabolic microphones, which often eliminate the need for for court-approved wiretaps.
- Closed circuit television cameras for visual surveillance.
- Automatic telephone switching equipment that records the time, length, origin and destination of telephone calls.
- Electronic beepers to track automobiles.
- Urine tests which detect past or current drug use.
- More lie detectors to assess employee honesty and discourage unauthorized leaks of information.
- Devices to monitor and intercept electronic mail.

The most alarming of the new surveillance technologies to privacy advocates lies in the computerized record systems of federal agencies.

Available information

The massive databases either contain or can acquire a person's medical and job histories, educational background, credit card purchases, bank transactions, tax payments, automobile records, applications for government aid, contributions to charity, subscriptions to publications and even library withdrawal records, among other things.

"Agencies can compile an electronic trail of where someone has been and what he has done," said professor George B. Trubow of the Center for Information Technology at John Marshall School of Law in Chicago. "The average person doesn't have slightest idea what is happening in the development of computer surveillance technology. In pursuing efficiency, agencies are putting things in place that have potential for enormous invasions of individual privacy," he added.

While MIT's Marx is concerned about a widespread "climate of suspiciousness," others fear that an outbreak of serious social or economic disruption could lead the government to mobilize the surveillance apparatus against dissident segments of society.

"That's not just idle speculation," said Jerry Berman, legislative counsel of the American Civil Liberties Union. "The technology is on line. The government can link its record systems together whenever it wants – whether to combat terrorism, subversion or even social deviance."

Most computerized record systems reside with agencies such as Health and Human Services, Social Security and Medicaid which deal with clients, as well as state and local goverments.

Computerized records

Government officials say computerized records enable them to better audit agency performance and to detect fraud by aid recipients. But critics say that, by comparing one agency's records against those of another – or against private records – agencies can use records for purposes other than auditing.

A growing number of databases are also used by law enforcement agencies. Last week, for example, defense officials attributed their success in arresting 13 Americans on espionage charges this year to the dramatic expansion of domestic surveillance.

According to the recent Office of Technology Assessment report, 85 computerized record systems used for law enforcement, investigative or intelligence purposes currently contain 288 million records on 114 million people. That represents half the population of the United States. And the figure does not include data held by the Central Intelligence, Defense Intelligence and National Security Agencies.

The FBI's National Crime Information Center is used by federal, state and local police nearly 400,000 times a day to check people stopped for traffic violations, as well as those suspected of serious crimes. It contains records on some 9 million people.

Yet, despite an FBI audit showing that the NCIC computer's responses include at least 12,000 invalid or inaccurate personal records each day, officials are currently proposing to expand those records to include files on white collar and organized crime and to use data from such quasi enforcement groups as campus and railroad police.

Continued

Growth of data exchange

That steady growth in the gathering and exchanging of data is "like the salami technique," said Trubow of the Marshall Law School. "No one slice hurts. But suddenly the whole sausage is gone. People can be kept under surveillance constantly by computers. It's a scenario for a very scary environment."

During the Carter administration, a proposal for a national database had to be withdrawn after intense opposition from critics concerned about the specter of "Big Brother".

But Mary Gerwin, an aide to Sen. William Cohen (R-Maine), noted that the current system of links between computerized files of federal, state and private agencies "presents the same kind of national databank that was opposed in the 1970s."

Gerwin is concerned about an administration proposal that would provide taxpayers' IRS records on unearned income to agencies which administer veterans' benefits, Pell college grants, guaranteed student loans, low-income housing aid, black lung benefits and federal employee benefits – programs that serve millions of citizens. The same proposal would also permit agencies to check the private individual and company-sponsored insurance records of all citizens.

"This isn't an infringement, and we are asking for very little in the way of records," Office of Management and Budget spokesman Steve Tupper said. "We're just asking for the states to do a little more checking because we're losing $300 million a year that's going out to the wrong people."

But the ACLU's Berman said the proposal "will result in a de facto national data center in which government agencies will be able to reach into hundreds of different computerized files and build a personal dossier on any man, woman or child who has been selected for examination."

In the last few years, critics have focused on such procedural remedies as due process for people identified by computers as, say, welfare cheats. Others want to amend the Privacy Act to limit Congressional authorization of computer matches.

But a recent ACLU position paper, citing the limitations of such piecemeal solutions, concluded that "we must change the terms of the debate to include these larger concerns about the society we are creating."

"Unfortunately," concluded Trubow, "Congress only responds to a clearly identified abuse. We don't have that right now. We're just laying the foundation for it.

"But when the abuse begins taking place, it's going to be too late to stop it," he said.